在BGP对等体之间配置MD5身份验证

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 网络图
- 配置
- 了解调试

验证

故障排除

相关信息

简介

本文档描述如何在两个 BGP 对等体之间的 TCP 连接上配置 Message Digest5 (MD5) 身份验证。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息基于运行Cisco IOS®版本12.4(15)T14的3600系列路由器的命令输出。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

您可以在两个BGP对等体之间配置MD5身份验证，这意味着将对对等体之间的TCP连接上发送的每个数据段进行验证。在两个 BGP 对等体上必须使用同一个口令配置 MD5 身份验证；否则，将无法建立它们之间的连接。配置MD5身份验证时，会使Cisco IOS软件生成并检查TCP连接上发送的每个数据段的MD5摘要。

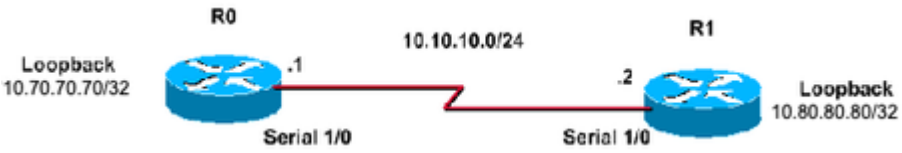
配置

本节介绍配置本文档所述功能的信息。

> 注意：使用Cisco CLI分析器获取有关本节中使用的命令的详细信息。只有注册的思科用户才能访问思科内部工具和信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

路由器 0 配置
<#root> R0# ! interface Loopback70

```
 ip address 10.70.70.70 255.255.255.255
!
interface Serial1/0
 ip address 10.10.10.1 255.255.255.0
 serial restart-delay 0
!
router bgp 400
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.80.80.80 remote-as 400



!--- iBGP Configuration using Loopback Address


 neighbor 10.80.80.80 password cisco



!--- Invoke MD5 authentication on a TCP connection to a BGP peer


 neighbor 10.80.80.80 update-source Loopback70
 no auto-summary
!
ip route 10.80.80.80 255.255.255.255 10.10.10.2


!--- This static route ensures that the remote peer address used for peering is reachable.
```

路由器 1 配置

<#root>

R1#

```
!
interface Loopback80
 ip address 10.80.80.80 255.255.255.255
!
interface Serial1/0
 ip address 10.10.10.2 255.255.255.0
 serial restart-delay 0
!
router bgp 400
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.70.70.70 remote-as 400


!--- iBGP Configuration using Loopback Address


 neighbor 10.70.70.70 password cisco


!--- Invoke MD5 authentication on a TCP connection to a BGP peer
```

```
 neighbor 10.70.70.70 update-source Loopback80
 no auto-summary
!
ip route 10.70.70.70 255.255.255.255 10.10.10.1


!--- This static route ensures that the remote peer address used for peering is reachable.
```

了解调试

<#root>

R0#

clear ip bgp *
*Mar 1 01:02:17.523: %BGP-5-ADJCHANGE: neighbor 10.80.80.80 Down User reset

<#root>

R0#

debug ip bgp

```
BGP debugging is on for address family: IPv4 Unicast
*Mar  1 01:03:58.159: BGP: 10.80.80.80 open failed: Connection timed out; remote host not responding, o
*Mar  1 01:03:58.415: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 01:03:59.943: BGP: 10.80.80.80 open active, local address 10.70.70.70
*Mar  1 01:04:00.039: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:00.807: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(33358) to 10.70.70.70(179)
*Mar  1 01:04:01.991: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:01.995: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:05.995: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:06.015: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:14.023: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:14.023: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:29.947: BGP: 10.80.80.80 open failed: Connection timed out; remote host not responding, o
*Mar  1 01:04:33.879: BGP: 10.80.80.80 open active, local address 10.70.70.70
*Mar  1 01:04:33.983: BGP: 10.80.80.80 went from Active to OpenSent
*Mar  1 01:04:33.983: BGP: 10.80.80.80 sending OPEN, version 4, my as: 400, hold time 180 seconds
*Mar  1 01:04:33.987: BGP: 10.80.80.80 send message type 1, length (incl. header ) 45
*Mar  1 01:04:34.091: BGP: 10.80.80.80 rcv message type 1, length (excl. header) 26
*Mar  1 01:04:34.091: BGP: 10.80.80.80 rcv OPEN, version 4, holdtime 180 seconds
*Mar  1 01:04:34.091: BGP: 10.80.80.80 rcv OPEN w/ OPTION parameter len: 16
*Mar  1 01:04:34.095: BGP: 10.80.80.80 rcvd OPEN w/ optional parameter type 2 (Capability) len 6
*Mar  1 01:04:34.095: BGP: 10.80.80.80 OPEN has CAPABILITY code: 1, length 4
*Mar  1 01:04:34.095: BGP: 10.80.80.80 OPEN has MP_EXT CAP for afi/safi: 1/1
*Mar  1 01:04:34.095: BGP: 10.80.80.80 rcvd OPEN w/ optional parameter type 2 (Capability) len 2
*Mar  1 01:04:34.095: BGP: 10.80.80.80 OPEN has CAPABILITY code: 128, length 0
*Mar  1 01:04:34.099: BGP: 10.80.80.80 OPEN has ROUTE-REFRESH capability(old) for all address-families
```

```
*Mar  1 01:04:34.099: BGP: 10.80.80.80 rcvd OPEN w/ optional parameter type 2 (Capability) len 2
*Mar  1 01:04:34.099: BGP: 10.80.80.80 OPEN has CAPABILITY code: 2, length 0
*Mar  1 01:04:34.099: BGP: 10.80.80.80 OPEN has ROUTE-REFRESH capability(new) for all address-families
*Mar  1 01:04:34.103: BGP: 10.80.80.80 went from OpenSent to OpenConfirm
*Mar  1 01:04:34.103: BGP: 10.80.80.80 went from OpenConfirm to Established
*Mar  1 01:04:34.103: %BGP-5-ADJCHANGE: neighbor 10.80.80.80 Up
```

如果一台路由器为邻居配置了密码，但是该邻居却没有为其配置密码，这种情况下，当这两台路由器尝试在它们之间建立 BGP 会话时，系统将显示如下消息：

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP address]:179
```

同样地，如果这两个路由器配置了不同的密码，系统将显示如下消息：

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:179
```

验证

使用本部分可确认配置能否正常运行。

- show ip bgp neighbors | include BGP

```
<#root>

R0#

show ip bgp neighbors| include BGP

BGP neighbor is 10.80.80.80

,

remote AS 400

, internal link
  BGP version 4, remote router ID 10.80.80.80

BGP state = Established

,

up for 00:08:26

  BGP table version 1, neighbor version 1/0
```

- show ip bgp summary

```
<#root>

R0#

show ip bgp summary

BGP router identifier 10.70.70.70, local AS number 400
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd

10.80.80.80 4 400 75 75 1 0 0 00:08:52 0
```

- show ip bgp summary

```
<#root>

R1#

show ip bgp summary

BGP router identifier 10.80.80.80, local AS number 400
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd

10.70.70.70 4 400 76 76 1 0 0 00:09:27 0
```

故障排除

当前没有此配置的故障排除信息。

相关信息

- 思科 IOS IP 路由：BGP 命令参考
- IP 路由支持页
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。